



Our Docket No: 42390P16424

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:)
)
Grobman, et al.)
)
Application No: 10/600,124)
)
Filed: June 20, 2003)
)
For: REMOTE DATA STORAGE)
VALIDATION)
_____)

Examiner: REZA, Mohammad W.

Art Unit: 2113

DECLARATION OF STEVEN L. GROBMAN
PURSUANT TO 37 C.F.R. §1.131

Sir:

I, Steven L. Grobman, hereby declare that:

1. I am the sole inventor of the above-referenced U.S. Patent application and of the subject matter described and claimed therein.

2. Intel Corporation, of Santa Clara, California, is the Assignee of the patent application described above.

3. I have been employed by Intel Corporation from prior to January 24, 2003.

4. At least prior to January 24, 2003, I conceived in this country (U.S.A.) the invention claimed in the above-described application.

5. As evidence of conception, attached hereto is Exhibit A, an Intel Invention Disclosure form (numbered 29945) entitled "Illicit Data Dumping Prevention in P2P Storage Partnerships." These pages are representative of my inventive work and were created at least as early as January 24, 2003.

6. Exhibit A describes a process that allows a first peer, who has stored backup data on a second peer, to perform a challenge/audit to determine if the second peer continues to preserve the backup data. This is particularly illustrated by a figure on the third page of Exhibit A.

7. The figure on the third page of Exhibit A illustrates peers negotiating a "partnership" to store each other's backup data. The peers exchange backup data. A first peer of the peers then initiates a challenge to a second of the peers to ensure that the second peer has not discarded the backup data. The first peer generates a key and then uses the key and the data to derive an MD5 checksum. The first peer sends the key to second peer. The second peer receives the key and uses the key and the backup data stored on the second peer to derive an MD5 checksum. The second peer sends its MD5 checksum to first peer. The first peer then determines whether there is a match between its MD5 checksum and the MD5 checksum sent by the second peer. If there is a match, then the second peer is still storing the backup data.


8. The *Teicher* reference (US Patent Application Publication 2004/0236958), filed on November 12, 2003, relies on Provisional Application No. 60/473,573, which was filed on May 25, 2003. From at least prior to May 25, 2003 to constructive reduction to practice (application filing on June 20, 2003), due diligence was taken in reducing the invention to practice.

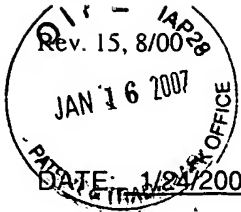
9. My diligence includes submission of the document attached as Exhibit A to the Intel Legal department for review, evaluation and selection for filing a U.S. Patent application, as well as work with patent attorney J. Scott Heilson to prepare the above-referenced U.S. Patent application for filing.

10. I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the above-described application or an patent issued therefrom.

Respectfully submitted,

Date 1/19, 2007


Steven L. Grobman



INTEL INVENTION DISCLOSURE
ATTORNEY-CLIENT PRIVILEGED COMMUNICATION
located at <http://legal.intel.com/patent/index.htm>

29945

SOFTWARE/FES/IT/GE

It is important to provide accurate and detailed information on this form. The information will be used to evaluate your invention for possible filing as a patent application. When completed and signed, please return this form to the **Legal Department at JF3-147**. You can submit electronically via e-mail to "invention disclosure submission" if all of the information is electronic, including drawings and supervisor approval. If you have any questions, please call 264-0444.

1. Inventor: Grobman Steven L
Last Name First Name Middle Initial
Phone 916-356-7467 M/S: FM1-102 Fax # _____
Citizenship: US WWID: 10069634 Contractor: YES _____ NO X
Inventor E-Mail Address: sgrobman@intel.com
Home Address: 1511 Southridge Ct
City El Dorado Hills State CA Zip 95762 Country USA
*Corporate Level Group (e.g. IAG, ICG, NBG) FES Division IT Subdivision GE
Supervisor* Alan Cross WWID 10026836 Phone 356-1012 M/S: FM1-102

Inventor: _____
Last Name First Name Middle Initial
Phone _____ M/S: _____ Fax # _____
Citizenship: _____ WWID: _____ Contractor: YES _____ NO _____
Inventor E-Mail Address: _____
Home Address: _____
City _____ State _____ Zip _____ Country _____
*Corporate Level Group (e.g. IAG, ICG, NBG) _____ Division _____ Subdivision _____
Supervisor* _____ WWID _____ Phone _____ M/S: _____

***If you are unsure of this information, please discuss with your manager.**

(PROVIDE SAME INFORMATION AS ABOVE FOR EACH ADDITIONAL INVENTOR)

2. Title of Invention: Illicit data dumping prevention in P2P storage partnerships
3. What technology/product/process (code name) does it relate to (be specific if you can):
Peer to peer storage partnership applications such as peer to peer backup solutions.
4. Include several key words to describe the technology area of the invention in addition to # 3 above: P2P, Storage
5. Stage of development (i.e. % complete, simulations done, test chips if any, etc.): Easily demonstrated in software
6. (a) Has a description of your invention been, or will it shortly be, published outside Intel:
NO: X YES: _____ If YES, was the manuscript submitted for pre-publication approval? _____
IDENTIFY THE PUBLICATION AND THE DATE PUBLISHED: _____
- (b) Has your invention been used/sold or planned to be used/sold by Intel or others?
NO: X YES: _____ DATE WAS OR WILL BE SOLD: _____

- (c) Does this invention relate to technology that is or will be covered by a SIG (special interest group)/standard/ or specification?

NO: X YES: _____ Name of SIG/Standard/Specification: _____

- (d) If the invention is embodied in a semiconductor device, actual or anticipated date of tapeout? No

- (e) If the invention is software, actual or anticipated date of any beta tests outside Intel No

7. Was the invention conceived or constructed in collaboration with anyone other than an Intel blue badge employee or in performance of a project involving entities other than Intel, e.g. government, other companies, universities or consortia? NO: X YES: _____ Name of individual or entity: _____

8. Is this invention related to any other invention disclosure that you have recently submitted? If so, please give the title and inventors: No

**PLEASE READ AND FOLLOW THE DIRECTIONS ON
 HOW TO WRITE A DESCRIPTION OF YOUR INVENTION**

Please attach a description of the invention to this form and include the following information:

1. **Describe in detail what the components of the invention are and how the invention works.**

Enables The Following Capability:

- Applications that negotiate peer to peer storage partnership relationships for backup purposes suffer from the problem that one partner can destroy the other partner's data to reclaim the resources used (as each partner has physical control of its hardware). This invention provides an efficient mechanism that enables a digital threat analogous to "I can easily tell if you still are holding my encrypted backup data and if not, I am going to destroy your backup data".

How the Invention Works (Simplest Scenario):

1. Each partner enters into the electronic agreement that allows them to store an encrypted "blob" on a partner in return for providing a similar service. Since the "blob" (hereafter meaning the encrypted data contents) is encrypted, the data itself cannot be obtained.
2. Generally, the "Blob" itself is not needed unless a data recovery is necessary. However, it is critical to ensure that the partner has not discarded the blob (in case it is required for recovery).
3. To prevent a partner from destroying the blob, a digital challenge can be made anytime that the partner is on the network (by either peer). The challenge places trivial amounts of data on the network and works as follows:
 - a) The challenger generates a random key and Prepends it to its copy of the encrypted blob (the challenger has its own blob unless it is in a recovery scenario).
 - b) An MD5 checksum (or similar) is generated from the random key plus the blob.
 - c) The challenger sends the random key to its partner who must perform the identical procedure.
 - d) The only way for the challenged partner to obtain the current key+blob checksum is to actually have the blob in its possession.
 - e) If the challenged partner has the blob it will return the accurate checksum to the challenging partner.
4. If a challenge fails (such as in the case where a partner can't respond to the challenge because it has discarded the blob), the challenging partner will terminate the partnership and discard its respective copy of the partners data.
5. If a challenge is successfully answered it should be noted that a second challenge is possible at any time and can only be correctly responded to if the data is not destroyed.

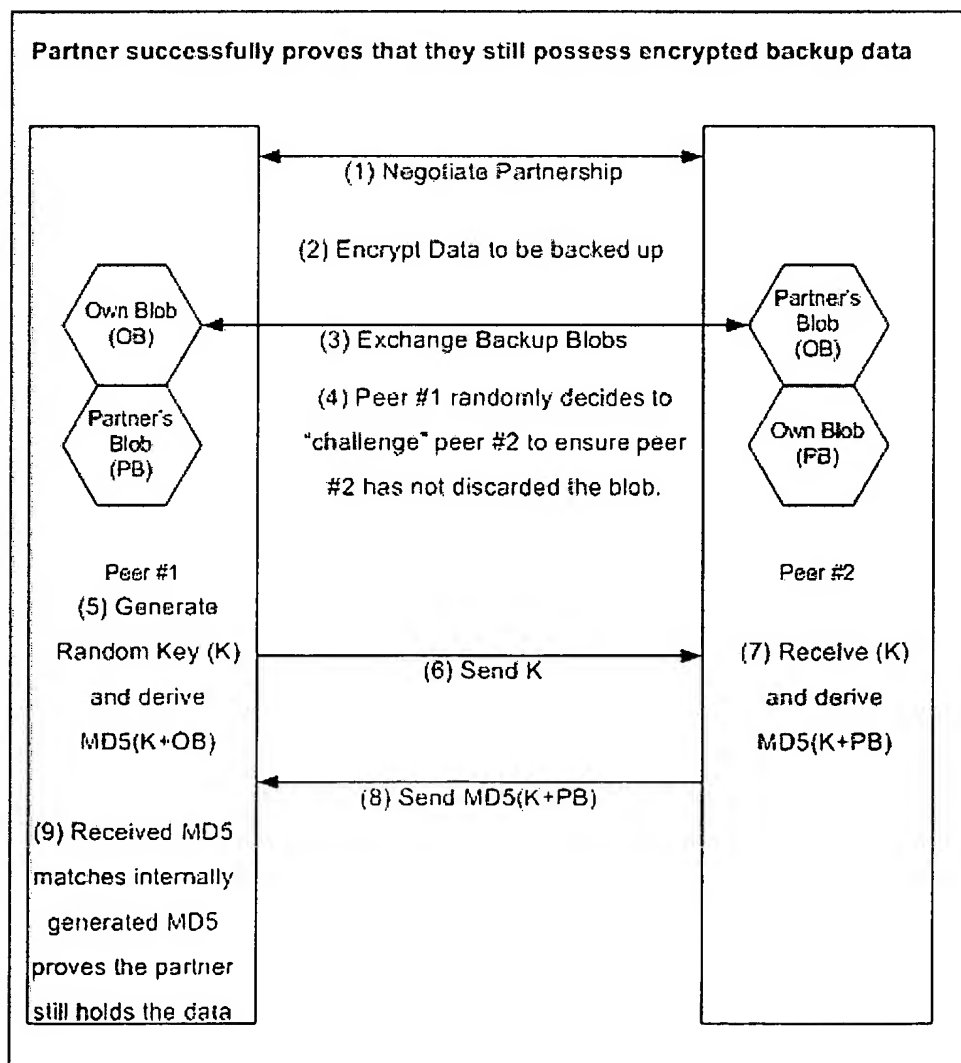
Additional Factors:

- Nothing prevents peers from hosting multiple partnerships to reduce the risk of data loss.
- A random key and resulting key+blob checksum can be generated immediately after the initial transfer to the partner which enables the client to not maintain a copy of its encrypted blob (to save space etc). The key and checksum are stored but not disclosed until a challenge is needed - the problem with this feature is that only one challenge is possible before the blob needs to be updated on the partner.
- Details such as partners disappearing from the network for extended duration invalidates a "contract" can be incorporated into the scheme.
- Nothing prevents this method from being used in non P2P situations such as a protocol to ensure that an ISP really is still storing a backup of critical files.

2. Describe advantage(s) of your invention over what is done now.

- In current P2P backup scenarios, there is nothing lost by not being a "team" player in a peer to peer relationship (such as by destroying a partners backup data). With this invention it is not possible to "play" in the peer network without "paying" by contributing to the P2P system.
- The challenge/audit is very light on network resources.
- In non P2P situations, it provides a mechanism to prove that a 3rd party backup provider really does have the content that they have agreed to store.

3. YOU MUST include at least one figure illustrating the invention.



4. Value of your invention to Intel (how will it be used?).

- Capability can be incorporated into both P2P file system schemes as well as products that ensure un-trusted 3rd parties are meeting their backup obligations (digital audit). Companies developing these capabilities can license this protocol/scheme.

5. Explain how your invention is novel. If the technology itself is not new, explain what makes it different.

- The invention is novel in that it solves the problem where users of a P2P backup solution delete the content that is enabling the overall capability (by doing so a user can't use the system).
- Introduces a new concept of a peer 2 peer digital "threat"
- Introduces a new concept of a "proof of life" or "proof of storage" in a P2P system.

6. Identify the closest or most pertinent prior art that you are aware of.

- Current P2P backup capabilities. For example:
<http://aip.intel.com/ATD/FSP/Storage/Projects/Peer2Peer/Research/MIT-LCS-TM-632.pdf>

7. Who is likely to want to use this invention or infringe the patent if one is obtained and how would infringement be detected?

Developers of P2P backup and file systems and backup solutions vendors are the primary parties that would infringe. Detection is straightforward by analyzing the protocol or features that the product offers.

**HAVE YOUR SUPERVISOR READ, DATE AND SIGN COMPLETED FORM
OR FORWARD IT ELECTRONICALLY VIA E-MAIL TO "INVENTION DISCLOSURE SUBMISSION"**

DATE: _____ SUPERVISOR: _____

BY THIS SIGNING, I (SUPERVISOR) ACKNOWLEDGE THAT I HAVE READ AND UNDERSTAND THIS DISCLOSURE, AND RECOMMEND THAT THE HONORARIUM BE PAID